CHAPTER

5

USERS, GROUPS, PROFILES, AND POLICIES

After reading this chapter and completing the exercises, you will be able to:

- Understand local users and groups
- Discuss the Windows 2000 Professional logon authentication
- Describe the default user accounts
- Establish a naming convention for accounts and groups
- Create and manage user accounts and profiles
- Understand local security policies

Many computers are used by more than one person, especially in business or educational environments. Each person is identified to the computer and ultimately the network through a unique user account and password. Typically, a **user account** contains details about the user, such as what he or she can and cannot access, and the preferred configuration or environmental settings. To establish such a system where details about each user are maintained, Windows 2000 uses named access accounts that are protected with password security. This chapter discusses these topics in detail.

WINDOWS 2000 PROFESSIONAL USER ACCOUNTS

Windows 2000 Professional is designed to be used as a network client for a Windows 2000 (and Windows NT) network or as a standalone operating system. From a Windows 2000 Professional system, you are only able to create, configure, and manage **local user accounts**. A local user account exists on a single computer. A local user account cannot be used in any manner with network resources or to gain network access of any kind. A local user account has absolutely no meaning to a domain or network. (A **domain** is an organizational unit used to centralize network users and resources.)

A **domain user account** exists in a domain by virtue of being created on a domain controller (a Windows 2000 Server). A domain user account exists throughout a domain and can be used on any computer that is a member of that domain. A domain user account is used to gain access to network resources. A domain user account can be used to grant access to local resources. Only Windows 2000 Servers can be domain controllers and create domain user accounts.

The information about user accounts and groups discussed in this chapter applies to local user accounts and local groups hosted by a Windows 2000 Professional system. Such local accounts can be maintained whether the host is a standalone desktop computer or a network client. When Windows 2000 Professional is a network client, it can assign access permissions to local resources used by domain groups, but it is unable to create domain groups or alter the membership of domain groups. It will be explicitly stated when material in this chapter applies to both local user accounts and domain user accounts. For more information on domain user accounts, see the Windows 2000 Server online Help, its related documentation, and the *Windows 2000 Server Resource Kit*.

On a Windows 2000 Professional system, whether acting as a client in a domain network or a peer-to-peer workgroup, or even as a standalone desktop system, user accounts are used to govern or control access. A Windows 2000 Professional system can:

- Be a standalone system where all users access local resources through a common user account that automatically logs on to the system upon bootup
- Be a standalone system where each user logs on to the system with a unique user account to gain access to local resources
- Be a network client where each user logs on to the system with a unique domain/network user account to gain access to network and local resources

A user account is used to uniquely identify a user to the system using a named user account and a password. Tied to this user account are numerous details about the user, including security settings and preferences. A Windows 2000 Professional local user account stores details about:

- *Security:* Passwords protect user accounts so only authorized individuals can gain access.
- *Access permissions:* User-specific settings and group memberships define the resources and applications a user has the authority to access and use.

- *Preferences:* A user's environmental settings and configuration preferences can be stored as a profile. If roaming profiles are enabled, the user's profile will be available from any computer on the network.

In addition to the preceding items, a Windows 2000 Professional system also maintains a wide range of security settings and preferences that affect a user account. These include password policy, account lockout policy, audit policy, user rights assignment, security options, public key policies, IP security policies, and more. Many of these topics are discussed later in this chapter.

Operating systems such as Windows 2000 that can support more than one user are called **multiple-user systems**. Maintaining a separate and distinct user account for each person is the common feature of all multiple-user systems. Windows 2000 implements its multiple-user system through the following:

- ***Groups***: Groups are named collections of users. Each member of a group takes on the access privileges or restrictions defined for that group. Through the use of groups, administrators can manage many users at one time because a group's settings can be defined once and apply to all members of that group. When the group settings are changed or modified, those changes automatically affect every member of that group. Thus, changing each user's account is not necessary. Later in this chapter, you will learn how to create and manage groups.
- ***Resources***: On a network or within a standalone computer, resources are any useful services or objects. This includes printers, shared directories, and software applications. A resource can be accessible by everyone across the network, or be limited to one person on a single machine, or be accessible or limited at any level in between. The range of control over resources within Windows 2000 is astounding. Details on how to manage resources and control who does have and who does not have access are presented later in this chapter.
- ***Policies***: A policy is a set of configuration options that defines aspects of Windows 2000 security. Security policies are used to define password restrictions, account lockouts, user rights, and event auditing. System policies are defined for a user, a computer, or a group to restrict the computing environment. Details on the different types of policies are discussed later in this chapter.
- ***Profiles***: A profile (sometimes called a **user profile**) is a stored snapshot of a user's desktop environment settings, Start menu, and other user-specific details. Profiles can exist on a single computer or can be configured to follow a user around a network, regardless of what workstation is used. User profiles are discussed in detail later in this chapter.

LOGGING ON TO WINDOWS 2000 PROFESSIONAL

Windows 2000 uses **logon authentication** (the requirement that a user provide a name and password to gain access to the computer) for two purposes: first, to maintain security and privacy within a network; and second, to track computer use by user account. Each Windows 2000 user can have a unique user account that identifies that user and contains or references all the system preferences for, access privileges of, and private information about that one user. Thus,Windows 2000 provides security and privacy for all users through the mandatory requirement of logon authentication.

> TIP
>
> In the instance of a standalone system where all users access local resources via common user accounts, logon still occurs; it just happens automatically.

Logon authentication is the simple process of entering a valid username and password to gain access to a Windows 2000-based computer. By pressing Ctrl+Alt+Delete at the default splash screen, the Logon Information dialog box appears. This is where users enter logon information—user name, password, and domain (optional)—and then click OK to have the security system validate their information and grant access to the computer. After users have completed their work, they can log off the computer (from Start, Shut Down, Logoff *username*) to make it available for the next user.

DEFAULT USER ACCOUNTS

When Windows 2000 Professional is installed, it automatically creates two default user accounts. These default accounts are Administrator and Guest.

Administrator

The Administrator account is the most powerful user account available in the Windows 2000 environment. This account has unlimited access and unrestricted privileges to every aspect of Windows 2000. The Administrator account also has unrestricted ability to manage all security settings, other users, groups, the operating system environment, printers, shares, and storage devices. Because of these far-reaching privileges, the Administrator account must be protected from misuse. Defining a complicated password for this account is highly recommended. You should also rename this account. This will make it more difficult for hackers to discover a valid user name and password.

The Administrator account has the following characteristics:

- It cannot be deleted.
- It cannot be **locked out** (disabled because of repeated failed logon attempts).
- It cannot be **disabled** (made unusable for logon).
- It cannot be removed from the Administrator's local group.
- It can be renamed.

TIP

It's always a good idea to rename the Administrator account to avoid giving away half of the user name/password combination to system attackers. Some administrators even suggest that you set up an account named Administrator, that has no access to the system, but has auditing enabled. By doing this, you not only lock down the most well-known user account, but you also can keep an eye on it in the event someone does try to attack your system using that account.

Guest

The Guest account is one of the least privileged user accounts in Windows 2000. This account has limited access to resources and computer activities. Even so, you should set a new password for the Guest account and it should be used only by authorized one-time users or users with low-security access. Any configuration changes made to the desktop or Start menu are not recorded in the Guest's user profile. If you do allow this account to be used, you should rename it.

The Guest account has the following characteristics:

- It cannot be deleted.
- It can be locked out.
- It can be disabled (it is disabled by default).
- It can have a blank password (it is blank by default).
- It can be renamed.

Naming Conventions

Before creating and managing user accounts, you need to understand naming conventions. A **naming convention** is simply a predetermined process for creating names on a network (or a standalone computer). A naming convention should incorporate a scheme for user accounts, computers, directories, network shares, printers, and servers. These names should be descriptive enough so anyone can decipher to which type of object the name corresponds. For example, name computers and resources by department or by use to simplify user access.

TIP

The stipulation of always using a naming convention may seem pointless for small networks, but it is rare for small networks to remain small. In fact, most networks grow at a staggering rate. If you begin naming network objects at random, you'll soon forget to which resource a name corresponds. Even with the excellent management tools of Windows 2000, you will quickly lose track of important resources if you have not established a standard method for naming network resources.

The naming convention on which your organization ultimately settles doesn't matter, as long as it can always provide you with a useful name for each new network object. To give you an idea of a naming scheme, two common rules follow:

- User names are constructed from the first and last name of the user, plus a code identifying his or her job title or department: for example, BobSmithAccounting or SmithBobAccounting.
- Group names are constructed from resource types, department names, location names, project names, and combinations of all four: for example, Accounting01, AustinUsers, BigProject01, etc.

Regardless of what naming convention is deployed, it needs to address the following four elements:

- It must be consistent across all objects.
- It must be easy to use and understand.
- New names should be easily constructed by mimicking the composition of existing names.
- An object's name should clearly identify that object's type.

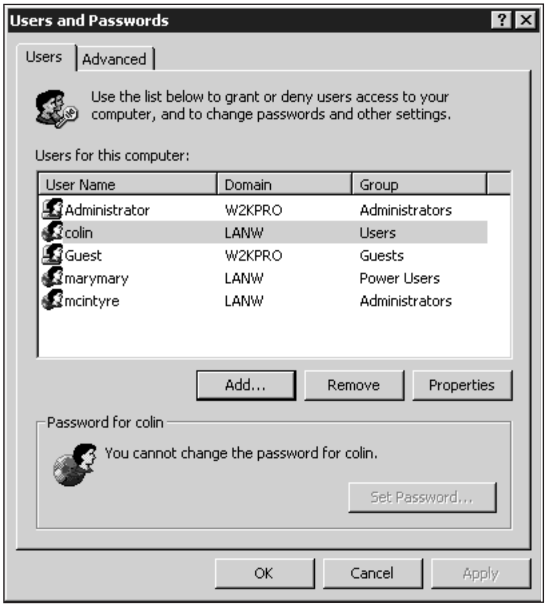
MANAGING USER ACCOUNTS

Windows 2000 Professional has two user account management tools. The first is the Users and Passwords applet accessed via the Control Panel. The second is the Local Users and Groups MMC snap-in accessed via the Advanced button on the Advanced tab of the Users and Passwords applet. The Users and Passwords applet is used to create a local user account from an existing domain account. The Local Users and Groups snap-in is used to create local user accounts from scratch.

Users and Passwords Applet

The Users and Passwords applet (see Figure 5-1) is used to perform several functions on local user accounts. This applet can be opened only if you are logged on to the Windows 2000 Professional system with the Administrator account, logged on with a user account which is a member of the Administrators group, or by providing the username, password, and domain when you attempt to launch the applet. This applet has two tabs: Users and Advanced. The Users tab displays all user accounts that can be employed to gain local access. This list details the user name, the domain (if the account is part of a domain; the screen differs for standalone computers), and the group memberships of the user account. The term *domain* in this instance refers to the logical environment where the user account originated. All user accounts created on the Windows 2000 Professional system have the local computer name listed as the domain (as in W2KPRO in Figure 5-1). All user accounts from a domain, such as accounts created by Windows 2000 Server, Windows NT Server, or another networking environment, will have the name of that domain listed as its domain (as in LANW in Figure 5-1).

To create new local user accounts, you must decide what type of user account to create. On a Windows 2000 Professional system, there are local user accounts created locally from scratch, and there are local user accounts that are local representations of domain or network user accounts. To create a new local user account from scratch, you need to employ the Local Users and Groups snap-in (see the next section). To create a local representation of an existing domain/network user account, use the Add button on the Users and Passwords applet. (Try Hands-on Project 5-1.)



Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

Users for this computer:

User Name	Domain	Group
Administrator	W2KPRO	Administrators
colin	LANW	Users
Guest	W2KPRO	Guests
marymary	LANW	Power Users
mcintyre	LANW	Administrators

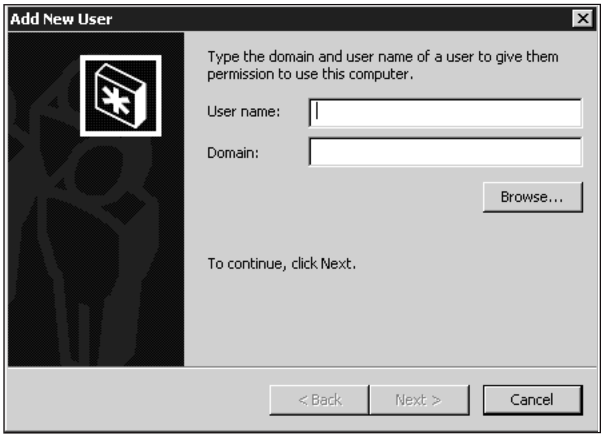
Password for colin

You cannot change the password for colin.

Figure 5-1 Users and Passwords applet

Creating a local representation of an existing domain/network user account grants a network user the ability to access resources hosted by the Windows 2000 Professional system, regardless of whether the system is a member of the domain/network. (This is possible because a workstation can exist on a network as a standalone system or as a workgroup member. Domain users can access resources on nondomain computers by viewing the shared items from the Entire Network via the My Network Places icon. For domain users to access resources, they must have a user account on the nondomain member Windows 2000 Professional system.) These **imported user accounts** cannot be used to log on to a Windows 2000 Professional system, but can be used only to access resources over the network hosted on a Windows 2000 Professional system. Plus, the use of local representations allows the administrator or user of a Windows 2000 Professional system to create a local security configuration of users and groups that does not rely upon the group memberships of the domain/network.

Clicking the Add button reveals the Add New User wizard (see Figure 5-2). If you know the name of the user account and the domain which it is from, you can type them in. You can also click the Browse button to see a list of existing user accounts in a domain. Clicking Next prompts you for the access level to grant the imported user (see Figure 5-3).



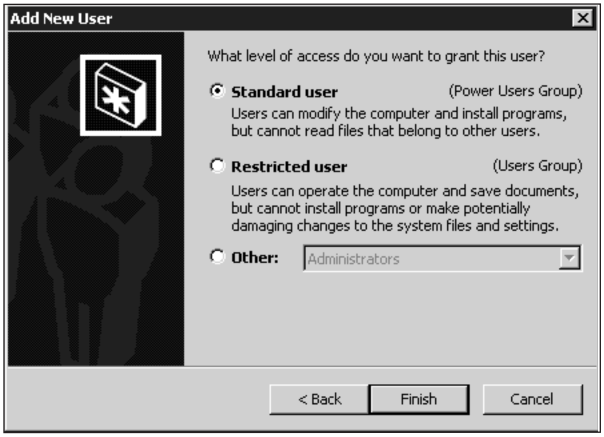
Type the domain and user name of a user to give them permission to use this computer.

User name:

Domain:

To continue, click Next.

Figure 5-2 Add New User wizard, user account and domain page



What level of access do you want to grant this user?

● **Standard user** (Power Users Group)
Users can modify the computer and install programs, but cannot read files that belong to other users.

○ **Restricted user** (Users Group)
Users can operate the computer and save documents, but cannot install programs or make potentially damaging changes to the system files and settings.

○ **Other:** Administrators

Figure 5-3 Add New User wizard, access level page

The access level to grant the imported user can be chosen from the following:

- *Standard user:* Grants the imported user membership into the Power Users group
- *Restricted user:* Grants the imported user membership into the Users group
- *Other:* Grants the imported user membership into the existing local group selected from the pull-down list

After you click Finish on the wizard, the imported user is added to the list of local users for this computer. To remove an existing user, just select it from the list and click Remove. You'll be prompted to confirm the user account deletion. (Try Hands-on Project 5-3.)

The Properties button on the Users and Passwords dialog box (shown earlier in Figure 5-1) is used to access basic properties for the selected user account. A locally created user account's Properties dialog box has two tabs: General and Group Membership. The General tab is used to change the user name, full name, and description. The Group Membership tab (which looks almost exactly like Figure 5-3) allows you to change a user's group membership. (Try Hands-on Project 5-2.) An imported user account's Properties has only a Group Membership tab, it does not have a General tab. An imported user account can be a member of only a single group. A locally created user account can be a member of more than one group, but the Group Membership tab of the Properties for the user account will allow only a single group to be selected and changed at a time. Adding a user account to multiple groups requires the use of the Local Users and Groups snap-in. Creating groups based on resources, then assigning users to multiple groups, you can create a permission scheme based solely on group permissions. This is advantageous because it is easier to manage group permissions than individual user permissions for every user on the network.

The password for locally created groups can be changed using the Set Password button at the bottom of the Users and Passwords applet (be sure to select the user account first). You will be prompted for the new password and a confirmation of the new password.

Imported user accounts appear in this applet whether or not the Windows 2000 Professional system is logged into the domain from which the accounts are imported. The only requirement is that the applet can communicate with the domain via a network connection. If the Windows 2000 Professional system is physically disconnected from the network media or the domain is not available, then the imported user accounts will not be listed. When the domain of origin returns, the user accounts will reappear.

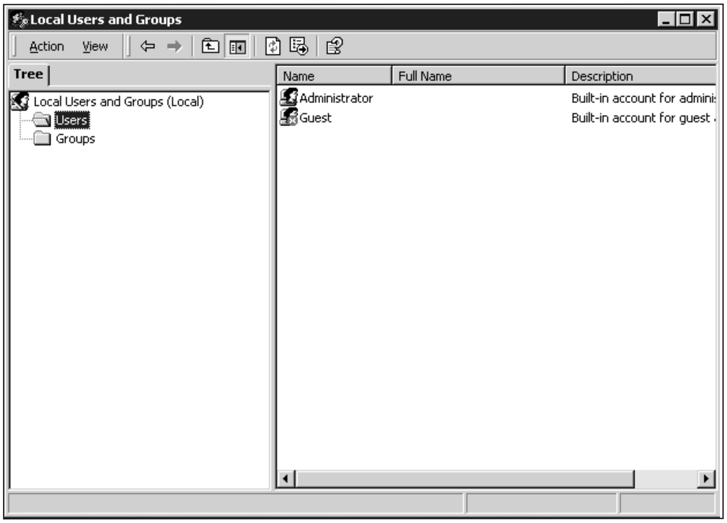
The Advanced tab of the Users and Password applet grants you access to certificate management, advanced user management, and secure boot settings. Certificate management is used to import and manage certificates that prove your identity as a user and certificate authority (certificate authorities are those organizations that verify your identity and assign you a certificate to use). Advanced user management is discussed in detail in the following section. Secure boot settings is a single check box that determines whether the Ctrl+Alt+Delete key sequence is required before the logon dialog box is displayed.

Local Users and Groups MMC Snap-in

The Local Users and Groups MMC snap-in (see Figure 5-4) is accessed by clicking the Advanced button on the Advanced tab of the Users and Passwords applet, or via a snap-in in the computer management console. This tool is used to create and manage local users only; imported users do not appear in this interface. (Practice creating a new local user account in Hands-on Project 5-4.) The console tree hosts two nodes: Users and Groups, shown as folders on the console screen. The Users folder contains all local user accounts. The Groups folder contains all local group accounts.

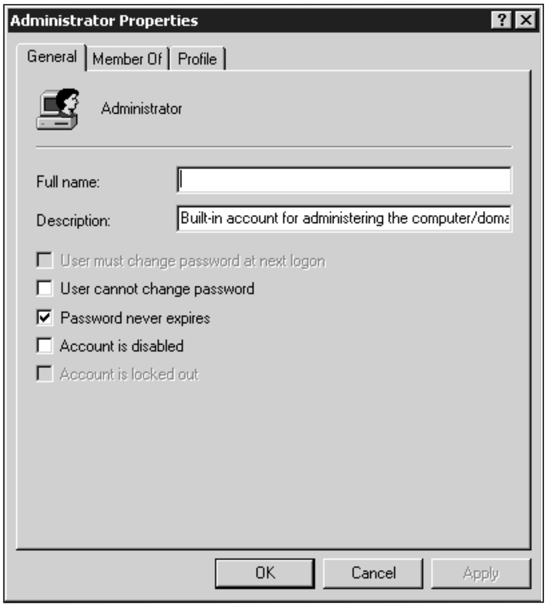
Users

Selecting the Users folder displays all existing local user accounts. When Windows 2000 Professional is first installed, only the Administrator and Guest accounts (as seen in Figure 5-4) will be displayed. The details pane on the right lists the name of the user account, the full name of the user, and the description of the account. By selecting a user account and right-clicking, you can access the account's Properties dialog box, which for a local user account has three tabs: General, Member Of, and Profile.



Name	Full Name	Description
Administrator		Built-in account for admini:
Guest		Built-in account for guest .

Figure 5-4 Local Users and Groups MMC snap-in



Full name:

Description: Built-in account for administering the computer/doma

□ User must change password at next logon

□ User cannot change password

☑ Password never expires

□ Account is disabled

□ Account is locked out

Figure 5-5 A user account's Properties dialog box, General tab

The General tab (see Figure 5-5) of a user account's Properties displays the following:

- *Name of user account*—Not customizable through this dialog box
- *Full Name*—Customizable full name of the person using the account
- *Description*—Customizable text field to describe the purpose or use of the account
- *User must change password at next logon*—A check box used to force a user to change their password the next time they log on to the system
- *User cannot change password*—A check box that prevents the user from altering the current password
- *Password never expires*—A check box that exempts this user from the account policy which defines the maximum lifetime of a password
- *Account is disabled*—A check box used to turn off an account, that prevents the account from being used, but retains it for security auditing purposes
- *Account is locked out*—A check box used by the lockout policy when an account meets the lockout parameters

The Member Of tab (see Figure 5-6) lists the groups of which this user account is currently a member. To add group memberships, click the Add button. This opens the Select Groups dialog box (see Figure 5-7). From this dialog box, you can select existing local groups to add this user account to. Select the group from the list and click Add. Once you've made your selections, click OK. To remove a group membership, select it on the Member Of tab and click Remove. (Try Hands-on Project 5-5 to change group membership for a local user account.)

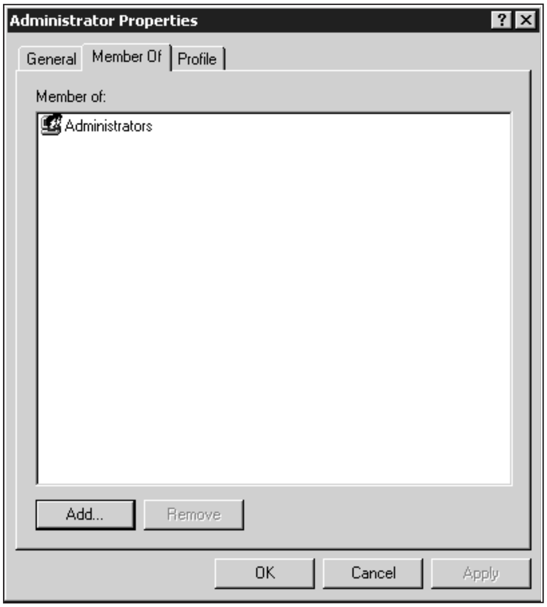
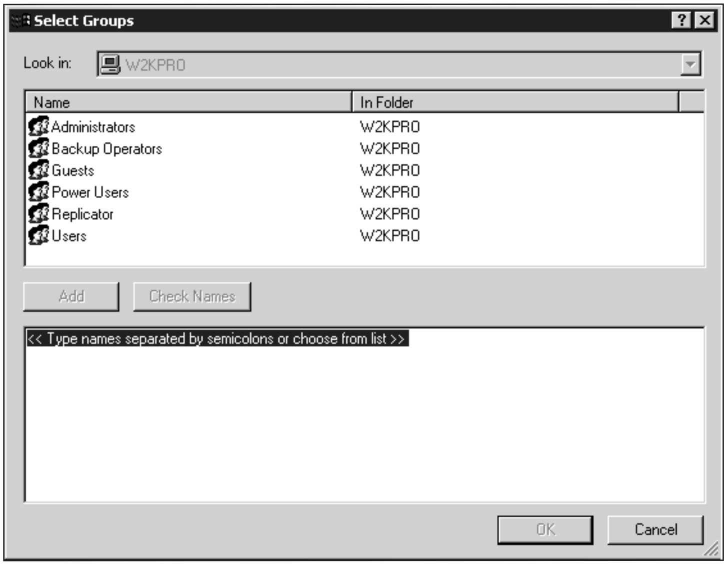


Figure 5-6 A user account's Properties dialog box, Member Of tab



Look in: W2KPRO

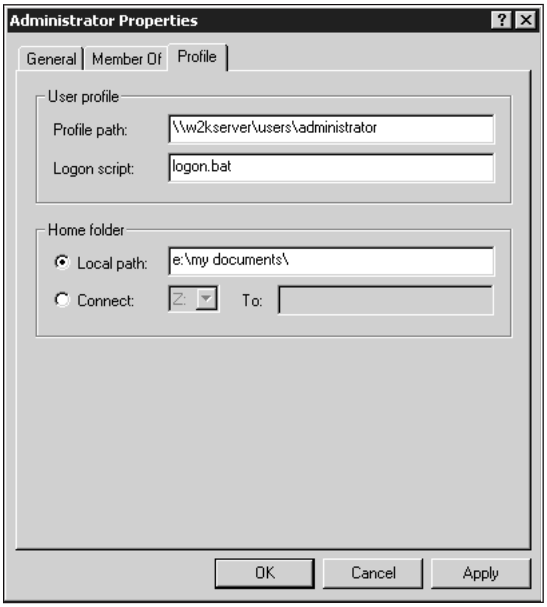
Name	In Folder
Administrators	W2KPRO
Backup Operators	W2KPRO
Guests	W2KPRO
Power Users	W2KPRO
Replicator	W2KPRO
Users	W2KPRO

<< Type names separated by semicolons or choose from list >>

Figure 5-7 Select Groups dialog box

The Profile tab (see Figure 5-8) is used to define the user profile path, logon script, and home folder. The Profile path designation defines the location where a user's profile will be stored. By default, user profiles are stored in partition system root\Documents and Settings\<*username*> where <*username*> is the name of the user to whom the profile belongs or applies. (User profiles are discussed in detail later in this chapter.) Logon script is the local path to a **logon script** which can map drive letters, launch applications, or perform other command-line operations each time the system boots. The home folder is the default location for the storage of user-created documents and files. By default, the home folder is the \Documents and Settings\<*username*>\My Documents folder, but this setting can be used to define an alternate location with either a path statement or with a mapped drive letter to a network share (such as K and \\mainserver\users\steve).

TIP For a Windows 2000 Professional local user, most of the paths used on the Profile tab should be local (that is, residing on the local computer).



Profile path: \\w2kserver\users\administrator

Logon script: logon.bat

● Local path: e:\my documents\

○ Connect: Z: To:

Figure 5-8 A user account's Properties dialog box, Profile tab

When you right-click a local user, the menu shows the Properties command, as well as four major commands:

- *Set Password*—Provide a new password and confirmation; the original password is not required.
- *Delete*—Completely removes a user account from the system; once deleted, it is not recoverable. Re-creating a new account, even with the same name and configuration, will be seen as a different account by the system because its SID (security identifier) will have changed.
- *Rename*—Change the name of the user account.
- *Help*—Access context-sensitive help.

Other local user account settings are defined through the **Local Security Policy** tool. Configuration options on a domain level are available in Windows 2000 Server.

Groups

Selecting the Groups node in the Local Users and Groups interface displays all existing local groups. As mentioned earlier, a group is a named collection of users. All members of a group share the privileges or restrictions of that group. Groups are used to give a specific level of access to multiple users through a single management action. Once a group has access to a resource, users can be added to or removed from that group as needed. The group concept is key to managing large numbers of users and their access to any number of resources. In fact, if you use the group concept effectively, there should be little need to assign access rights to an individual user.

A local user can be a member of multiple groups. Different groups can be assigned different levels of access to the same resources. In most cases, the most permissive of all granted access levels will be used, except when access is specifically denied by one or more groups.

As you plan your network security, user base, and resource allocation, remember to keep in mind how you will manage each of these groups. Think about how groups can be paired with resources to provide you with the greatest range of administrative control. After your resources are in place and all the required groups have been created, most of your administrative tasks will involve adding users to or removing them from these groups. This is mostly a concern when setting up Windows 2000 Server, but you should keep it in mind when planning any part of a network.

To provide the highest degree of control over resources, Windows 2000 uses two types of groups: local and global. **Local groups** exist only on the computer where they are created. **Global groups** exist throughout a domain. Windows 2000 Professional can create and manage local groups. Windows 2000 Professional can add only existing global groups to its local groups to grant access to resources. This distinction is very important, as you'll soon see. Local groups can have members who are users or global groups. Global groups can have only users from the domain in which they reside as members.

One of the differences between Windows 2000 Server and Windows 2000 Professional is that the user account and group tools on a Windows 2000 Professional system can manage local users and local groups. To create and manage groups across domains, you must have a Windows 2000 Server in a client/server environment. The Active Directory Users and Computers interface on Windows 2000 Server is used to create and manage domain users, global groups, and local groups. If a Windows 2000 Professional system is part of a domain, its user tools can add global groups to local groups as members, but that is the only activity it can perform with global groups.

With local and global groups, a complete system of links from resources to users can be established. Each resource is assigned to one or more local groups. Users are assigned to one or more global groups in their domains. Global user groups are assigned to local resource groups. Each local group can be assigned different levels or types of access to the resource. By placing a global group in a local group, you assign all members of that global group the privileges of the local group, that is, access to a resource. In other words, on a domain scale, domain users are members of global groups, which in turn are members of local groups that are assigned access permissions to resources. On a local computer, local users are members of local groups which are assigned access permissions to resources.

TIP

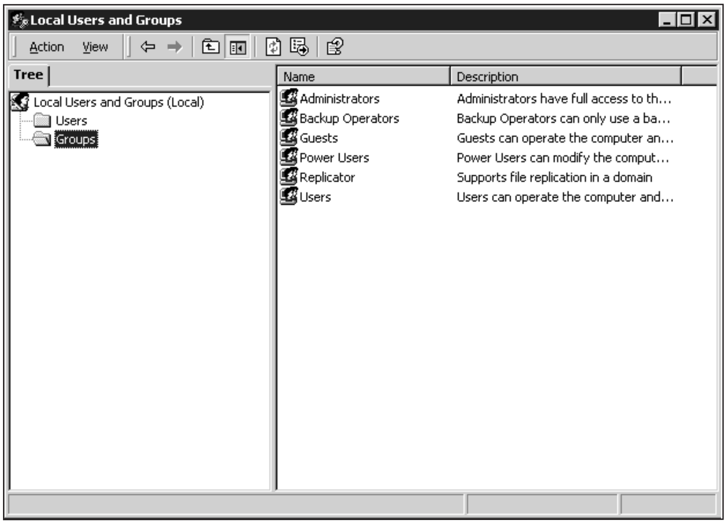
It is important to understand the distinction between local and global groups: local groups can contain members that are users or global groups, whereas global groups can only have users from the domain in which they reside as members. When you assign access permissions to resources, you assign those rights to local groups.

You must plan your group management scheme long before you begin implementation. Planning such a scheme involves applying a naming scheme, dividing users into meaningful groups, and understanding the various levels of access your resources offer. For the group method to be effective, you need to manage all access to resources through groups. Never succumb to the temptation to assign access privileges directly to a user account.

Defining group members is often the most time-consuming process of group management. A group should be formed around a common job position, need of resource, or even geographic location. Some existing groups you can transform into Windows 2000 groups are:

- Organizational functioning units, workgroups, or departments
- Authorized users of network programs and applications
- Events, projects, or special assignments
- Authorized users of network resources
- Location or geography
- Individual function or job description

As stated, local groups exist only on the computer where they are created. On each computer, all local groups must have a unique name. You can duplicate the names of local groups on different computers, but they will be separate and distinct groups. Avoid using the same name twice on any network, even if the architecture allows you to do so.



Name	Description
Administrators	Administrators have full access to th...
Backup Operators	Backup Operators can only use a ba...
Guests	Guests can operate the computer an...
Power Users	Power Users can modify the comput...
Replicator	Supports file replication in a domain
Users	Users can operate the computer and...

Figure 5-9 Local Users and Groups, Groups folder

Windows 2000 Professional has six default groups. When the Groups node is selected in the Local Users and Groups interface, these default groups (as seen in Figure 5-9) will be displayed:

- *Administrators:* Members of this group have full access to the computer. Default members are the Administrator account and the Domain Admins group if connected to a domain.
- *Backup Operators:* Members of this group can back up and restore all files and folders on a system. It has no default members.
- *Guests:* Members can operate the computer and save files, but cannot install programs or alter system settings. Default member is the Guest account.
- *Power Users:* Members can modify the computer, create user accounts, share resources, and install programs, but cannot access files that belong to other users. It has no default members.
- *Replicator:* This group is used by special user accounts to facilitate file synchronization between systems and domains. It has no default members. For more information about data synchronization, see the *Windows 2000 Resource Kit*.
- *Users:* Members can operate the computer and save files, but cannot install programs, modify user accounts, share resources, or alter system settings. Default members are the Authenticated Users group (a nonconfigurable default group) and the Domain Users group if connected to a domain. By default, Windows 2000 adds all new local user accounts to this group.

New groups are created using the New Group command. (Try Hands-on Project 5-6.) When creating a new group, you need to provide the group name and a description, and add members.

The Properties dialog box for a user group allows you to change its description and alter its membership. You can add members to a group from the list of local user accounts or from the list of domain user accounts. Imported user accounts are not listed in this interface. Groups can also be deleted (see Hands-on Project 5-7) or renamed by selecting the command from the right-click pop-up menu or from the Action menu.

System Groups

Windows 2000 Professional has several built-in system-controlled groups. System groups are preexisting groups that you cannot manage, but which appear in dialog boxes when assigned group membership or access permissions. These groups are:

- *Everyone:* Includes all users accessing the computer, both defined local user accounts and imported accounts. Assign access to the Everyone group with caution because it also includes the Guest account and anonymous logons (such as with Web and FTP servers).
- *Authenticated Users:* Includes all users with a specifically defined local user account, except for the Guest account
- *Creator Owner:* Includes the user account of the current owner of an object

- *Network:* Includes all user accounts accessing the computer over a network connection
- *Interactive:* Includes the user account of the person currently logged into the local system
- *Anonymous Logon:* Any user account that did not go through official authentication by the Windows 2000 security system
- *Dialup:* Includes any user account accessing the computer over a dial-up connection

USER PROFILES

A user profile is the collection of desktop and environmental configurations on a Windows 2000 system for a specific user or group of users. By default, each Windows 2000 computer maintains a profile for each user who has logged on to the computer, except for Guest accounts. Each user profile contains information about a particular user's Windows 2000 configuration. Much of this information is about things the user can set, such as color scheme, screen savers, and mouse and keyboard layout. Other information covers settings that are accessible only to a Windows 2000 administrator, such as access rights to common program groups or network printers.

The material stored in a user profile includes:

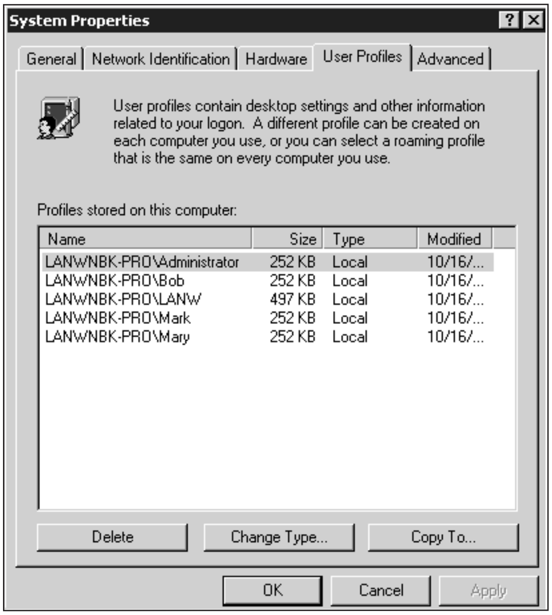
- *Application Data*—A directory containing user-specific data, such as for Internet Explorer or Outlook
- *Cookies*—A directory containing cookies (cookies are text scripts that a Web browser sends to a server to customize a user's browsing experience) accepted by the user via their browser
- *Desktop*—A directory containing the icons displayed on the user's desktop
- *Favorites*—A directory containing the user's list of URLs from Internet Explorer
- *Local Settings*—A directory containing user-specific history information and temporary files
- *My Documents*—A directory containing user-created data
- *NetHood*—A directory containing user-specific network mappings
- *PrintHood*—A directory containing user-specific printer mappings
- *Recent*—A directory containing user-specific links to the last accessed resources
- *Sent To*—A directory containing user-specific links used in the Sent To command of the right-click pop-up menu
- *Start Menu*—A directory containing the user-specific Start menu layout
- *Templates*—A directory containing user-specific Microsoft Office templates
- *Ntuser.dat*—A file containing user-specific Registry information

- *Ntuser.dat.log*—A transaction log file that ensures the user profile can be re-created in the event of a failure
- *Ntuser.ini*—A file containing profile-related settings, such as what directories should not be uploaded to a roaming profile

Optionally, an administrator can force users to load a so-called **mandatory profile**. Users can adjust this profile while they're logged in, but all changes are lost as soon as they log out.

> A mandatory profile is created by manually renaming the Ntuser.dat file to Ntuser.man. This technique provides a way for administrators to control the look and feel of shared accounts, or to restrict nonpower users from exercising too much influence over their desktops.

User profiles are managed through the User Profiles tab that appears in the System applet. This tab (see Figure 5-10) lists all profiles for users who have logged into the Windows 2000 Professional system under examination. The dialog box displays the name of the user account, along with defining its domain of origin, the disk space consumed by the profile, the profile type, and when it was last changed. Profiles can be two types: local or roaming.



User profiles contain desktop settings and other information related to your logon. A different profile can be created on each computer you use, or you can select a roaming profile that is the same on every computer you use.

Profiles stored on this computer:

Name	Size	Type	Modified
LANWNBK-PRO\Administrator	252 KB	Local	10/16/...
LANWNBK-PRO\Bob	252 KB	Local	10/16/...
LANWNBK-PRO\LANW	497 KB	Local	10/16/...
LANWNBK-PRO\Mark	252 KB	Local	10/16/...
LANWNBK-PRO\Mary	252 KB	Local	10/16/...

Figure 5-10 System applet, User Profiles tab

Local Profiles

A **local profile** is a set of specifications and preferences for an individual user, stored on a local machine. Windows 2000 provides each user with a folder containing their profile settings. Individual profiles are stored in the system partition root\Documents and Settings folder. A different location for the Profiles folder can be specified through the Local Users and Groups tool.

Local profiles are established by default for each user who logs on to a particular machine, and reside in the *%username%* subfolder beneath the system partition root\Documents and Settings folder. Although it may seem inevitable that an explicit user profile management utility would exist for Windows 2000, user profiles really represent a specialized snapshot of a user's preferences, desktop configuration, and related settings.

There is no single tool that permits all user profile information to be manipulated abstractly. There are only two ways to create a user profile:

- A user logs on and arranges things as needed, and upon logout this information will become that user's local profile (which may then be transformed into a roaming profile as you'll learn later),
- Assign a mandatory profile to a user from an existing definition (but even this must be set up by example, rather than through explicit controls).

Windows 2000 Professional local users (including imported users) have only local profiles. It is not possible to transform a local user's local profile to a roaming profile. However, a domain user account that logs on to a Windows 2000 Professional system will have a local profile created the first time they log on (assuming they do not already have a roaming profile on the network). This local profile for the domain user can be transformed into a roaming profile.

Roaming Profiles

A **roaming profile** resides on a network server to make it broadly accessible. When a user whose profile is designated as roaming logs on to any Windows 2000 system on the network, that profile is automatically downloaded when the user logs on. This avoids having to store a local profile on each workstation that a user uses, but it also has a disadvantage. If a user's roaming profile is large, logging on to the network takes quite a while because that information must be copied across the network each time the user logs in.

The default path designation for a roaming profile is *\\computername\username*. To create a roaming profile, use the "Copy to" button that appears in the User Profile tab of the System applet on a machine where a local profile for the user already exists. The destination for the copy operation must match the path that defines where the roaming profile resides (as manually defined in the user account). (This is the profile path shown in Figure 5-8.) The Profile path is defined either on the local computer for local accounts, or on a domain controller for domain accounts. The path is the mechanism that tells the startup module where to find a user's roaming profile. Local profiles are always stored in the system partition\Documents and Settings folder and do not require setting a profile path in the user account properties. Roaming profiles, however, require you to specify a path to the network profile share.

TIP

Keep in mind that only domain accounts can use roaming profiles. Once a local profile is present on a client, such as a Windows 2000 Professional system, you must use the System applet on that system to copy the profile to a network file server. Then, you must access the Active Directory Users and Computers tool on a Windows 2000 Server machine to alter the profile path for the domain user account.

Local Security Policy

Windows 2000 has combined several security and access controls into a centralized policy. This centralized policy is called the group policy. A **group policy** is an MMC snap-in that is used to specify users' desktop settings. There are group policies for local computers, groups, and domains, and **organizational units (OUs)**. (An organizational unit is an administrative container object that can contain users, groups, resources, and other OUs).

All group policy types can be managed from a Windows 2000 Server system, but only a local computer group policy can be managed from a Windows 2000 Professional system.

Group policies are applied in the following order:

1. Any existing legacy Windows NT 4.0 Ntconfig.pol file is applied.
2. Any unique local group policy is applied (that is, the group policy for the local machine).
3. Any site group policies are applied.
4. Any domain group policies are applied.
5. Any OU group policies are applied.

The order of application of these policies is important because contradictory settings in later policies will override the settings of the former policies. The cumulative result of this priority application of group policy is known as the **effective policy**. On Windows 2000 Professional systems, the effective policy is either all of these group policies properly combined when logged on with a domain user account, or only the local group policy when logged on with a local user account.

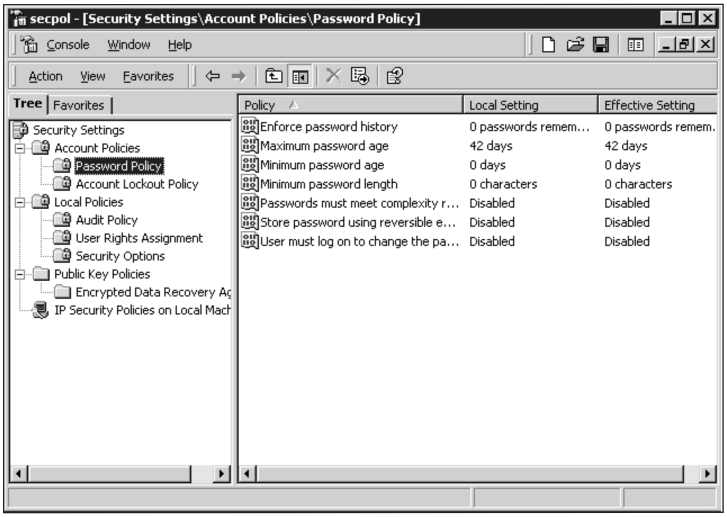
The Local Security Policy tool is used to edit the local group policy on a Windows 2000 Professional system. This tool is accessed from the Administrative Tools applet from the Control Panel. (Try Hands-on Project 5-8.) The local group policy consists of several subpolicies, including: password, account lockout, audit, user rights, security options, public key, and IP security.

TIP

Notice in the details section of the MMC snap-in tool that each specific policy item is listed with both its local setting and its effective setting. Local settings apply only when logged in with a local user account. Effective settings apply when logged in with a domain user account. For all policy items, only the local default setting is listed because the effective setting varies based on network configuration.

Password Policy

The **password policy** defines the restrictions on passwords, as shown in Figure 5-11. This policy is used to enforce strong passwords for a more secure environment. By using a password policy, you can assign any of the items listed in Table 5-1 to a user to force the user to use a certain type of password.



secpol - [Security Settings\Account Policies\Password Policy]

Policy	Local Setting	Effective Setting
Enforce password history	0 passwords remem...	0 passwords remem.
Maximum password age	42 days	42 days
Minimum password age	0 days	0 days
Minimum password length	0 characters	0 characters
Passwords must meet complexity r...	Disabled	Disabled
Store password using reversible e...	Disabled	Disabled
User must log on to change the pa...	Disabled	Disabled

Figure 5-11 Local Security Policy, Password Policy

Table 5-1 Password Policy Items and Their Descriptions

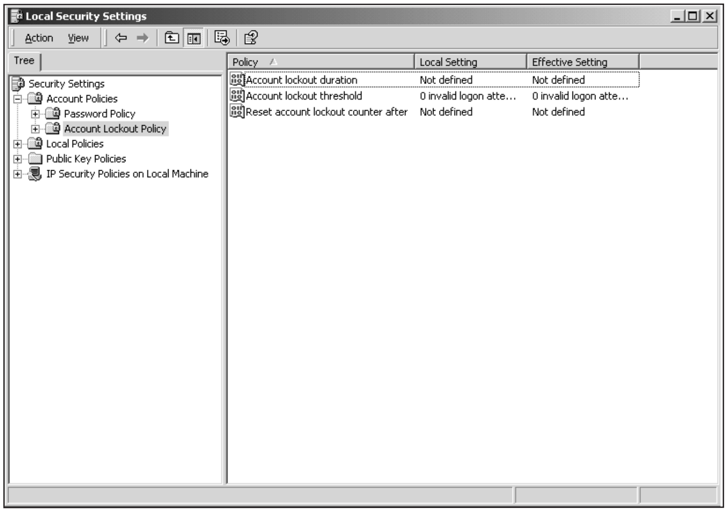
Policy Item: Default Setting	Description
Enforce password history: 0 Passwords	Maintaining a password history prevents reuse of old passwords. A setting of 5 or greater for this item is recommended.
Maximum password age: 42 days	Defines when passwords expire and must be replaced. A setting of 30, 45, or 60 days is recommended.
Minimum password age: 0 days	Defines the least amount of time that can pass between password changes. A setting of 1, 3, or 5 days is recommended.
Minimum password length: 0 characters	Sets the minimum number of characters that must be present in a password. A setting of 6 or more is recommended.
Passwords must meet complexity requirements of installed password filter: Disabled	Determines whether passwords must comply with installed password filters. See the *Windows 2000 Resource Kit* for details.

Table 5-1 Password Policy Items and Their Descriptions (continued)

Policy Item: Default Setting	Description
Store passwords using reversible encryption for all users in the domain: Disabled	Determines whether SPAP (Shiva Password Authentication Protocol) is used to encrypt passwords. Leave this disabled unless required by a client.

Account Lockout Policy

The **account lockout policy** defines the conditions that result in a user account being locked out. Figure 5-12 shows the Account Policy Lockout dialog box, which is accessed from the Local Security Policy tool of the Administration tools. Lockout is used to prevent brute force attacks against user accounts. For example, if a user tries to log on and is unsuccessful more than five (or the specified number) times, it's a good idea to lock that user out. Then the user must get assistance from an administrator to gain access to the system. If the person attempting to gain access is not a valid user, they will not be able to log on to the system using that user name.



Policy	Local Setting	Effective Setting
Account lockout duration	Not defined	Not defined
Account lockout threshold	0 invalid logon atte...	0 invalid logon atte...
Reset account lockout counter after	Not defined	Not defined

Figure 5-12 Local Security Policy, Account Lockout Policy

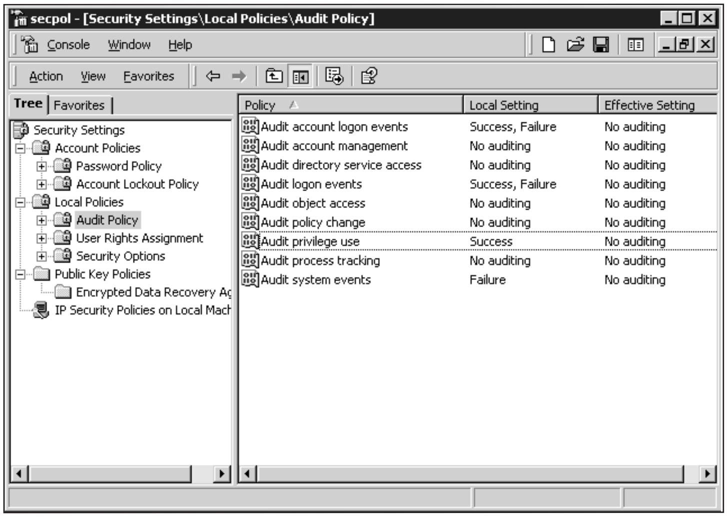
The items in this policy are:

- *Account lockout threshold: 0 Invalid logon attempts*—Defines the number of failed logons that must occur before an account is locked out. A setting of 3 to 5 is recommended.
- *Account lockout duration: Not Defined*—Defines the length of time an account will remain locked out. A value of 0 will cause locked out accounts to require administrative action to unlock. A setting of 30 minutes to 2 hours is recommended.

- *Reset account lockout counter after: Not Defined*—Defines the length of time that must expire before the failed logon attempts counter for a user account is reset. A setting of 15 minutes is recommended.

Audit Policy

The **audit policy** defines the events that are recorded in the Security log of the Event Viewer. The audit policy is configured in the Audit Policy dialog box shown in Figure 5-13. Auditing tracks the use and misuse of resources. Take, for example, the recommendation earlier in this chapter to create a fake Administrator account. If someone were to try to use that account to gain access to the system, you could track those attempts and know when someone was trying to attack your system. You then could take additional preventative measures. Each item in this list can be set to audit the Success and/or Failure of the event.



Policy	Local Setting	Effective Setting
Audit account logon events	Success, Failure	No auditing
Audit account management	No auditing	No auditing
Audit directory service access	No auditing	No auditing
Audit logon events	Success, Failure	No auditing
Audit object access	No auditing	No auditing
Audit policy change	No auditing	No auditing
Audit privilege use	Success	No auditing
Audit process tracking	No auditing	No auditing
Audit system events	Failure	No auditing

Figure 5-13 Local Security Policy, Audit Policy

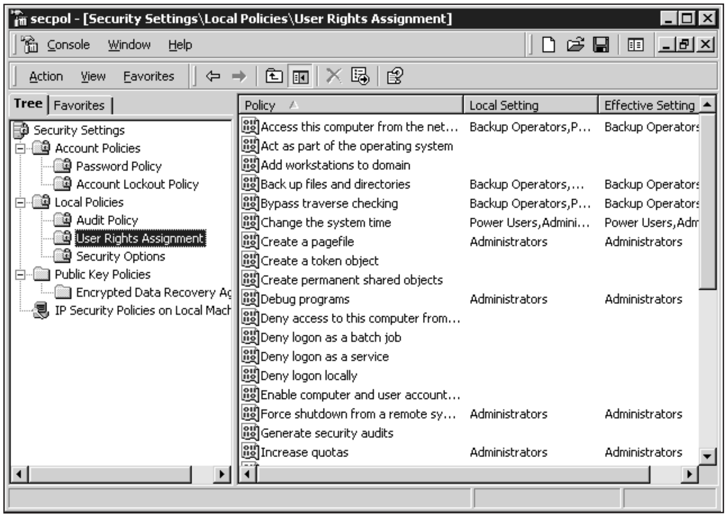
The items in this policy are:

- *Audit account logon events*—Audits the logon and logoff of user accounts
- *Audit account management*—Audits the changes to user accounts and group memberships
- *Audit directory service access*—Audits access to network resources
- *Audit logon events*—Audits nonuser account logon and logoff events
- *Audit object access*—Audits resource access
- *Audit policy change*—Audits changes to the security policy
- *Audit privilege use*—Audits use of special rights or privileges

- *Audit process tracking*—Audits the activity of processes
- *Audit system events*—Audits system-level activities

User Rights Policy

The **User Rights Policy** defines which groups or users can perform specific privileged actions (see Figure 5-14). For example, you may want to give a group, such as Power Users, the right to add a workstation to a domain.



Policy	Local Setting	Effective Setting
Access this computer from the net...	Backup Operators,P...	Backup Operators
Act as part of the operating system		
Add workstations to domain		
Back up files and directories	Backup Operators,...	Backup Operators
Bypass traverse checking	Backup Operators,P...	Backup Operators
Change the system time	Power Users,Admini...	Power Users,Adm
Create a pagefile	Administrators	Administrators
Create a token object		
Create permanent shared objects		
Debug programs	Administrators	Administrators
Deny access to this computer from...		
Deny logon as a batch job		
Deny logon as a service		
Deny logon locally		
Enable computer and user account...		
Force shutdown from a remote sy...	Administrators	Administrators
Generate security audits		
Increase quotas	Administrators	Administrators

Figure 5-14 Local Security Policy, User Rights Assignment

The items in this policy and their default settings are:

- *Access this computer from the network*—Everyone, Users, Power Users, Backup Operators, Administrators
- *Act as part of the operating system*—none
- *Add workstations to domain*—none
- *Back up files and directories*—Backup Operators, Administrators
- *Bypass traverse checking*—Everyone, Users, Power Users, Backup Operators, Administrators
- *Change the system time*—Power Users, Administrators
- *Create a pagefile*—Administrators
- *Create a token object*—none
- *Create permanent shared objects*—none
- *Debug programs: Administrators*

- *Deny access to this computer from the network*—none
- *Deny logon as a batch job*—none
- *Deny logon as a service*—none
- *Deny logon locally*—none
- *Enable computer and user accounts to be trusted for delegation*—none
- *Force shutdown from a remote system*—Administrators
- *Generate security audits*—none
- *Increase quotas*—Administrators
- *Increase scheduling priority*—Administrators
- *Load and unload device drivers*—Administrators
- *Lock pages in memory*—none
- *Log on as a batch job*—none
- *Log on as a service*—none
- *Log on locally*—Guests, Users, Power Users, Backup Operators, Administrators
- *Manage auditing and security log*—Administrators
- *Modify firmware environment values*—Administrators
- *Profile single process*—Power Users, Administrators
- *Profile system performance*—Administrators
- *Remove computer from docking station*—Users, Power Users, Administrators
- *Replace a process-level token*—none
- *Restore files and directories*—Backup Operators, Administrators
- *Shut down the system*—Users, Power Users, Backup Operators, Administrators
- *Synchronize directory service data*—none
- *Take ownership of files or other objects*—Administrators

User Rights are enabled as defined in the previous list by default. You can alter this configuration via the User Rights Assignment section of the Local Security Policy (try Hands-on Project 5-8).

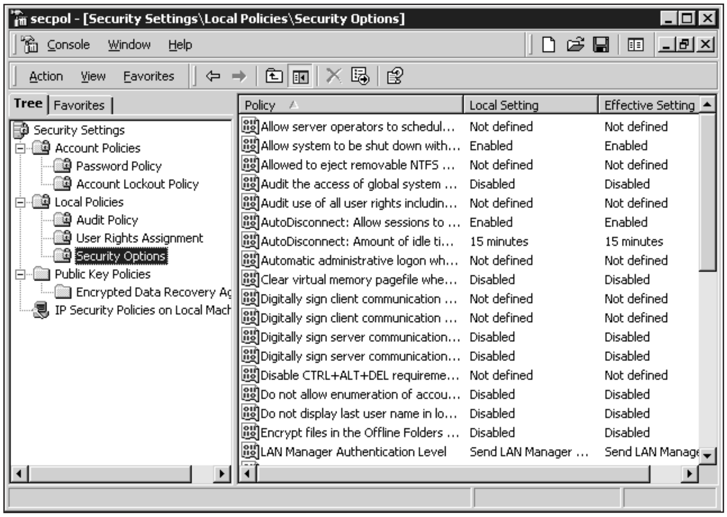
TIP

Troubleshooting user rights involves testing access to or control of resources, reconfiguring rights as needed, and retesting. If you suspect an action cannot be performed that should be possible, test, reset the associated user right, relog on as that user, and try the action again. Be sure to double-check any file or object permissions associated with the action because it may be blocked by lack of access rather than a user right.

TIP For more details on these security options, please consult the *Windows 2000 Professional Resource Kit*.

Security Options

The **security options** define and control various security features, functions, and controls of the Windows 2000 environment (see Figure 5-15). For example, you can disable the option to allow the system to be shut down without having to log on to tighten security. The items in this policy and their default settings are described in Table 5-2.


secpol - [Security Settings\Local Policies\Security Options]
Console
Window
Help
Action
View
Favorites
Tree
Favorites

- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Public Key Policies
    - Encrypted Data Recovery Ag
  - IP Security Policies on Local Mach

Policy	Local Setting	Effective Setting
Allow server operators to schedul...	Not defined	Not defined
Allow system to be shut down with...	Enabled	Enabled
Allowed to eject removable NTFS ...	Not defined	Not defined
Audit the access of global system ...	Disabled	Disabled
Audit use of all user rights includin...	Not defined	Not defined
AutoDisconnect: Allow sessions to ...	Enabled	Enabled
AutoDisconnect: Amount of idle ti...	15 minutes	15 minutes
Automatic administrative logon wh...	Not defined	Not defined
Clear virtual memory pagefile whe...	Disabled	Disabled
Digitally sign client communication ...	Not defined	Not defined
Digitally sign client communication ...	Not defined	Not defined
Digitally sign server communication...	Disabled	Disabled
Digitally sign server communication...	Disabled	Disabled
Disable CTRL+ALT+DEL requireme...	Not defined	Not defined
Do not allow enumeration of accou...	Disabled	Disabled
Do not display last user name in lo...	Disabled	Disabled
Encrypt files in the Offline Folders ...	Disabled	Disabled
LAN Manager Authentication Level	Send LAN Manager ...	Send LAN Manage

Figure 5-15 Local Security Policy, Security Options

Table 5-2 Security Options and Their Default Settings

Security Option	Default Setting
Additional restrictions for anonymous connections	None. Rely on default permissions
Allow server operators to schedule tasks (domain controllers only)	Not defined
Allow system to be shut down without having to log on	Enabled
Allow to eject removable NTFS media	Administrators
Amount of idle time required before disconnecting session	15 minutes
Audit the access of global system objects	Disabled
Audit use of Backup and Restore privilege	Disabled
Automatically log off users when logon time expires (local)	Enabled
Clear virtual memory pagefile when system shuts down	Disabled

Table 5-2 Security Options and Their Default Settings (continued)

Security Option	Default Setting
Digitally sign client communication (always)	Disabled
Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (always)	Disabled
Digitally sign server communication (when possible)	Disabled
Disable CTRL+ALT+DEL requirement for logon	Not defined
Do not display last user name in logon screen	Disabled
LAN Manager Authentication Level	Send LAN Manager and NTLM responses
Message text for users attempting to log on	blank
Message title for users attempting to log on	blank
Number of previous logons to cache (in case domain controller is not available)	10 logons
Prevent system maintenance of computer account password	Disabled
Prevent users from installing printer drivers	Disabled
Prompt user to change password before expiration	14 days
Recovery Console: Allow automatic administrative logon	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled
Rename administrator account	Not defined
Rename guest account	Not defined
Restrict CD-ROM access to locally logged-on user only	Disabled
Restrict floppy access to locally logged-on user only	Disabled
Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Disabled
Send unencrypted password to connect to third-party SMB servers	Disabled
Shut down system immediately if unable to log security audits	Disabled
Smart card removal behavior	No Action
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled
Unsigned driver installation behavior	Not defined
Unsigned non-driver installation behavior	Not defined

TIP For more details on these security options, please consult the *Windows 2000 Professional Resource Kit*.

CHAPTER SUMMARY

- This chapter discussed local users and groups. Windows 2000 Professional can employ three types of users: locally created users, imported users, and domain users. A user account stores security and preference settings for each person who uses a computer. Each user can have their own profile that retains all of their preferred desktop settings. Users are collected into groups to simplify management and grant access or privileges.

- Users and groups are managed through the Users and Passwords applet and the Local Users and Groups MMC snap-in. Windows 2000 Professional has two built-in users, Administrator and Guest, and several built-in groups. Some groups allow you to customize their membership whereas others are system-controlled groups whose memberships cannot be customized.

- User profiles can be local profiles when working with local users or imported users, or they can be roaming when using a domain user account. User profiles store a wide variety of personalized or custom data about a user's environment. A user profile can be mandatory just by changing Ntuser.dat to Ntuser.man.

- The Local Security Policy is used to manage passwords, account lockouts, audits, user rights, security options, and more. These controls aid in enforcing security and controlling who is able to perform specific actions on the system.

KEY TERMS

account lockout policy — Defines the conditions that result in a user account being locked out.

audit policy — Defines the events which are recorded in the Security log of the Event Viewer.

disabled — The state of a user account which is retained on the system but cannot be used to log on.

domain — An organizational unit used to centralize network users and resources.

domain user account — A user account which can be used throughout a domain.

effective policy — The cumulative result of the priority application of group policies.

global group — A group which exists throughout a domain. A global group can be created only on a Windows 2000 Server system.

group policy — An MMC snap-in that is used to specify desktop settings for group members.

groups — Named collections of users to which you assign permissions. For example, the Administrators group contains all users who require administrative access to network resources and user accounts.

imported user account — A local account created by duplicating the name and password of an existing domain account. An imported account can be used only when the Windows 2000 Professional system is able to communicate with the domain of the original account.

local group — A group which exists only on the computer where it was created. A local group can have users and global groups as members.

local profile — A set of specifications and preferences for an individual user stored on a local machine.

Local Security Policy — The centralized control mechanism which governs password, account lockout, audit, user rights, security options, public key, and IP security.

local user account — A user account that exists on a single computer.

locked out — The state of a user account that is disabled because of repeated failed logon attempts.

logon authentication — The requirement to provide a name and password to gain access to the computer.

logon script — A code script that can map drive letters, launch applications, or perform other command-line operations each time the system boots.

mandatory profile — A user profile which does not retain changes after the user logs out. Mandatory profiles are used to maintain a common desktop environment for users.

multiple-user system — An operating system which maintains separate and distinct user accounts for each person.

naming convention — A standardized regular method of creating names for objects, users, computers, groups, etc.

organizational unit (OU) — A container object that is an administrative partition of the Active Directory. OUs can contain users, groups, resources, and other OUs. OUs enable the delegation of administration to distinct subtrees of the directory.

password policy — Defines the restrictions on passwords.

policy — A set of configuration options that defines aspects of Windows 2000 security.

profile — See user profile.

resources — Any useful service or object on a network. This includes printers, shared directories, and software applications. A resource can be accessible by everyone across the network or by only one person on a single machine, and at any level in between.

roaming profile — A profile that resides on a network server to make it broadly accessible. When a user whose profile is designated as roaming logs on to any Windows 2000 system on the network, that profile is automatically downloaded when the user logs on.

security options — Define and control various security features, functions, and controls of the Windows 2000 environment.

user account — A named security element used by a computer system to identify individuals and to record activity, control access, and retain settings.

user profile — A collection of user-specific settings that retain the state of the desktop, start menu, color scheme, and other environmental aspects across logons. By default, user profiles are stored in system partition root\Documents and Settings\<*username*>, where *username* is the name of the user to whom the profile applies.

User Rights Policy — Defines which groups or users can perform the specific privileged action.

REVIEW QUESTIONS

1. What types of user accounts can Windows 2000 Professional create and manage? (Choose all that apply.)
   a. local
   b. domain
   c. imported
   d. global
2. What types of user accounts can be used on a Windows 2000 Professional system? (Choose all that apply.)
   a. local
   b. domain
   c. imported
   d. global
3. When not connected to a network, what types of user accounts can be employed on a Windows 2000 Professional system?
   a. local
   b. domain
   c. imported
   d. global

4. A multiuser system is an operating system that allows more than one user account to log on to a single workstation simultaneously. True or False?
5. Which of the following are true of groups? (Choose all that apply.)
   a. Several default groups are built into Windows 2000.
   b. Groups are named collections of users.
   c. The system groups can be deleted through the Local Users and Groups tool.
   d. Groups used to simplify the assignment of permissions.
6. Why does Windows 2000 require logon authentication? (Choose all that apply.)
   a. to prevent the spread of viruses
   b. to track computer usage by user account
   c. to maintain security
   d. to promote a naming scheme
7. Which of the following are true for both the Administrator account and the Guest account? (Choose all that apply.)
   a. cannot be deleted
   b. can be locked out
   c. cannot be disabled
   d. can be renamed
8. When logged in under the Guest account, a user has the same access as other members of what group?
   a. Authenticated Users
   b. Users
   c. Power Users
   d. Everyone
9. Through what interface are imported user accounts managed?
   a. User Manager for Domains
   b. Users and Passwords
   c. Local Users and Groups
   d. Active Directory Users and Computers
10. Which of the following are true of imported users? (Choose all that apply.)
    a. can be a member of only a single group
    b. you can change their password
    c. exist only when their domain of origin is present online
    d. are used to grant domain users access to the local resources

11. When creating a new user via the Users and Passwords applet, the Restricted user selection makes the new user a member of what group?
    a. Guests
    b. Power Users
    c. Users
    d. Backup Operators
12. To configure more than one group membership for a local user account requires the use of the Users and Passwords applet. True or False?
13. When the control item under Secure boot on the Advanced tab of the Users and Passwords applet is selected, not only is Ctrl+Alt+Delete not required, but the last user account to successfully log on will be automatically reused to log on to the system. True or False?
14. You create several new user accounts. You tell everyone they need to log on and change their password to something other than the dummy "password" you entered to create the account. In the past most users forget or refuse to change the password. What setting can you use to force them to make this change?
    a. user cannot change password
    b. user must change password at next logon
    c. password never expires
    d. account is disabled
15. On a Windows 2000 Professional client, what types of profiles can be used? (Choose all that apply.)
    a. Local
    b. Roaming
    c. Mandatory
    d. Dynamic
16. User profiles are stored by default in a subdirectory named after the user account in what default directory on a Windows 2000 Professional system?
    a. \Winnt\Profiles
    b. \Users
    c. \Profiles
    d. \Documents and Settings
17. The user account Properties dialog box from the Local Users and Groups tool can be used to change the password. True or False?
18. The user tools of Windows 2000 Professional can create and manage both local and global groups. True or False?
19. Local groups can have global groups as members. True or False?

20. Which of the following groups are not configurable? (Choose all that apply.)
    a. Administrators
    b. Interactive
    c. Backup Operators
    d. Creator Owner
    e. Authenticated Users
21. What makes a profile mandatory?
    a. check box setting via the user account's Properties dialog box
    b. storing it locally
    c. renaming a file with the extension .man
    d. not connecting to a network
22. The effective policy is the result of applying all network or domain hosted security policies, then applying the local security policy. True or False?
23. The local security policy is a collection of what individual policies? (Choose all that apply.)
    a. Password
    b. Account lockout
    c. Audit
    d. User rights
    e. Security options
    f. Public key
    g. IP security
24. To prevent malicious users from breaking into your computer system by repeatedly trying to guess a password, what built-in security tool can you use?
    a. Password policy
    b. IP security
    c. Lockout
    d. Encryption
25. What control element in Windows 2000 is used to assign specific privileged actions to users and groups?
    a. Auditing
    b. User rights
    c. Profiles
    d. Security options

HANDS-ON PROJECTS

Project 5-1

To import a user account:

TIP This hands-on project requires that a domain be accessible over a network connection.

1. Open the **Control Panel** (**Start**, **Settings**, **Control Panel**).
2. Open the **Users and Passwords** applet (double-click its icon).
3. Click **Add**.
4. In the **Add New User** wizard, click **Browse**.
5. Select a user account from the list, and then click **OK**.
6. Click **Next**.
7. Select **Standard User** when prompted about the level of access to grant this user, and then click **Finish**.
8. Notice the imported user appears in the list of users on the Users and Passwords applet.
9. Click **OK** to close the applet.

Project 5-2

To change group membership of an imported user:

TIP This project requires that Hands-on Project 5-1 be completed.

1. In the **Users and Passwords** applet, select the imported user you created in Hands-on Project 5-1.
2. Click **Properties**.
3. Select the **Other** radio button on the **Group Membership** tab.
4. From the pull-down list, select **Power Users**.
5. Click **OK**.

Project 5-3

To delete a user account:

1. In the **Users and Passwords** applet, select the imported user created in Hands-on Project 5-1.
2. Click **Remove**.
3. When asked to confirm, click **Yes**.

Project 5-4

To create a new local user account:

1. Select the **Advanced** tab on the **Users and Passwords** applet.
2. Click the **Advanced** button.
3. Select the **Users** node in the console tree of **Local Users and Groups**.
4. From the Action menu, select **New User**.
5. In the New User dialog box, enter a user name (such as "BobTemp"), full name (such as "Bob Smith"), and description (such as "A temporary account for Bob").
6. Provide a password and a confirmation of that password.
7. Deselect the **User must change password at next logon** option.
8. Click **Create**.
9. Click **Close**.
10. The BobTemp user account will now be listed in the details pane.

Project 5-5

To change group membership for a local user account:

> TIP This project requires that Hands-on Project 5-4 be completed.

1. Select the BobTemp user account you created in Hands-on Project 5-4.
2. Select **Properties** from the Action menu.
3. Select the **Member Of** tab.
4. Click the **Add** button.
5. Select the **Power Users** group.
6. Click **Add**.
7. Click **OK**.
8. Select the **Users** group.

9. Click **Remove**.
10. Click **OK** to close the **Properties** dialog box.

Project 5-6

To create a local group:

TIP This project requires that Hands-on Project 5-4 be completed.

1. Select the **Groups** node in the console tree.
2. Select the **New Group** command from the Action menu.
3. In the **New Group** dialog box, provide a name (such as "SalesGrp") and a description (such as "members of the sales department").
4. Click **Add**.
5. Select the **BobTemp** user.
6. Click **Add**.
7. Click **OK**.
8. Click **Create**.
9. Click **Close**.

Project 5-7

To delete a group:

TIP This project requires that Hands-on Project 5-6 be completed.

1. Select the **SalesGrp** you created in Hands-on Project 5-6.
2. Select **Delete** from the **Action** menu.
3. When prompted to confirm, click **Yes**.
4. Close the **Local Users and Groups** tool by clicking the **X** button in the upper-right corner of the title bar.
5. Close the **Users and Passwords** applet by clicking **OK**.

Project 5-8

To change the Local Security Policy:

1. If not already open, open the **Control Panel** (**Start**, **Settings**, **Control Panel**).
2. Open the **Administrative Tools** applet (double-click its icon).

3. Open the **Local Security Policy** applet (double-click its icon).
4. Expand the **Account Policies** node (click the plus sign beside the node).
5. Select the **Password Policy** node.
6. Select **Enforce password history**.
7. Select the **Security** command from the Action menu.
8. In the setting dialog box, set the value to **5**.
9. Click **OK**.
10. Select **Maximum password age**.
11. Select the **Security** command from the Action menu.
12. In the setting dialog box, set the value to **60**.
13. Click **OK**.
14. Select **Minimum password age**.
15. Select the **Security** command from the Action menu.
16. In the setting dialog box, set the value to **2**.
17. Click **OK**.
18. Select **Minimum password length**.
19. Select the **Security** command from the Action menu.
20. In the setting dialog box, set the value to **6**.
21. Click **OK**.
22. Select the **Account Lockout Policy** node.
23. Select **Account lockout threshold**.
24. Select the **Security** command from the Action menu.
25. In the setting dialog box, set the value to **3**.
26. Click **OK**, then click **OK** again.
27. Select **Account lockout duration**.
28. Select the **Security** command from the Action menu.
29. In the setting dialog box, set the value to **30** (if it is not already set to 30).
30. Click **OK**.
31. Select **Reset account lockout counter after**.
32. Select the **Security** command from the Action menu.
33. In the setting dialog box, set the value to **15**.
34. Click **OK**.
35. Expand the **Local Policies** node (click the plus sign beside the node).
36. Select the **Audit Policy** node.
37. Select **Audit logon events**.

38. Select the **Security** command from the Action menu.
39. In the setting dialog box, select **Failure**.
40. Click **OK**.
41. Select **Audit system events**.
42. Select the **Security** command from the Action menu.
43. In the setting dialog box, select **Success and Failure**.
44. Click **OK**.
45. Close all open windows.

Project 5-9

To change user rights:

1. Open the Control Panel by selecting **Start**, **Settings**, **Control Panel**.
2. Double-click the **Administrative Tools** icon.
3. Double-click the **Local Security Policy** icon.
4. Double-click the **Local Policies** node.
5. Select **User Rights Assignment**.
6. Double-click **Add workstations to domain**.
7. Click **Add**.
8. Locate and select **Power Users**.
9. Click **Add**.
10. Click OK.
11. Click OK.
12. Close the Local Security Settings dialog box.

Case Projects

1. Your notebook computer is attached to a docking station whenever you are in the office. Although your Windows 2000 Professional notebook does not become a member of the domain when docked, it does have the ability to communicate with the domain. Your docking station hosts a color slide printer. How can you grant access to the printer to domain users when your notebook is docked?
2. You are concerned about file security. Recently a staff member was reprimanded because he restored files to a FAT partition instead of to an NTFS partition. The user account is a member of the Backup Administrators group and the Power Users group. Because FAT does not have file level security, the settings on the files allowed everyone on the network to view the confidential files. How can you change the Local Security Policy to prevent this from occurring in the future?